Lifecycle Management

Sandra L. Prior, REM, CHMM

System Safety and Safety Systems for Accelerators

US Particle Accelerator School

June 28 – July 2, 2004

Outline

- Overview of Safety Lifecycle
- Objective
  - Introduce the concept of a safety lifecycle and the applicability and context in safety systems.

Lifecycle Management

- A risk based management plan for a system or subsystem from conception to decommissioning.

(and recommissioning)

ISA 84.01 Definition

IEC 61508 Definition

Safety Lifecycle (IEC 61508)

necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.

IEC 61511 Definition

Safety Lifecycle (IEC 61511)

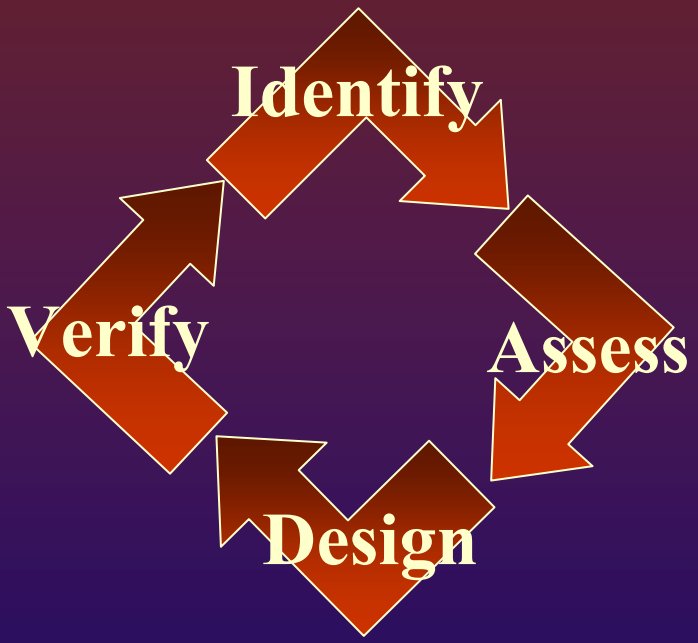
necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use

MIL-STD-882d Definition

‘ Life cycle. All phases of the system's life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal.’

MIL-STD-882d

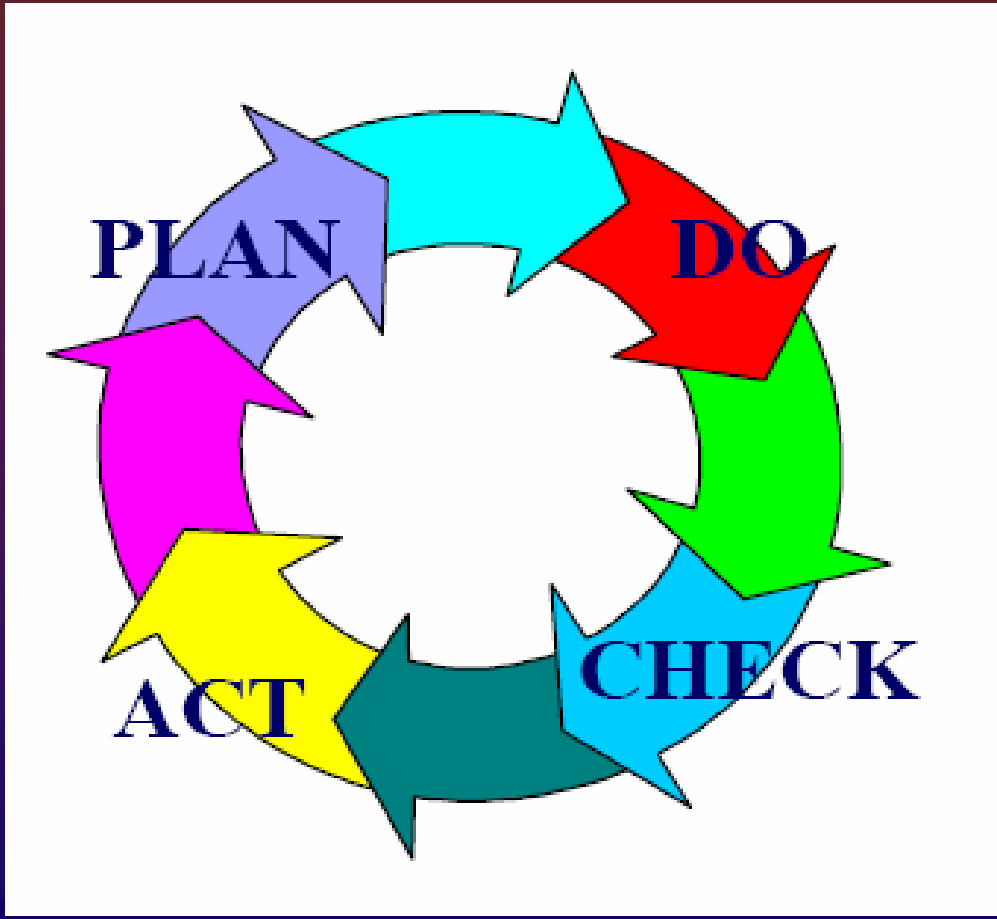
Safety Lifecycle Approach



The safety lifecycle approach, as described in ISA 84.01, IEC 61511, and IEC 61508:

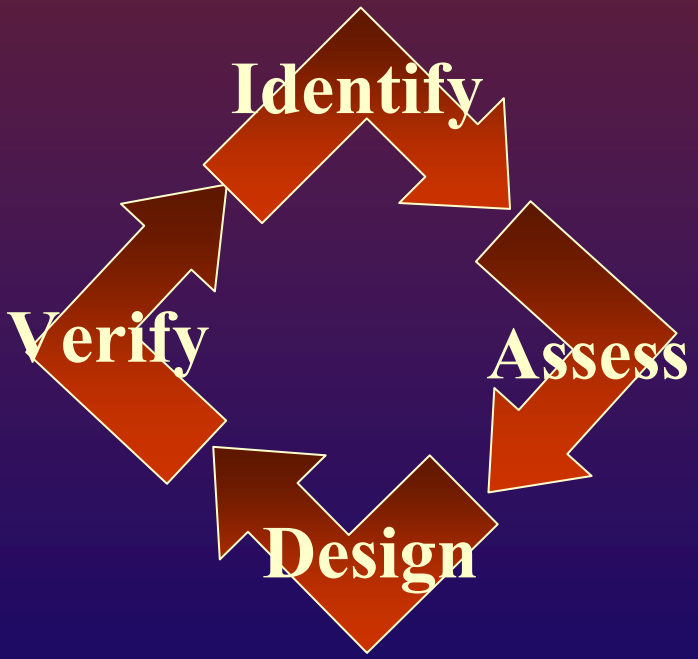
- ✓utilizes common sense
- ✓is a closed loop process
- ✓Is continuous/has no end

Quality Systems Approach

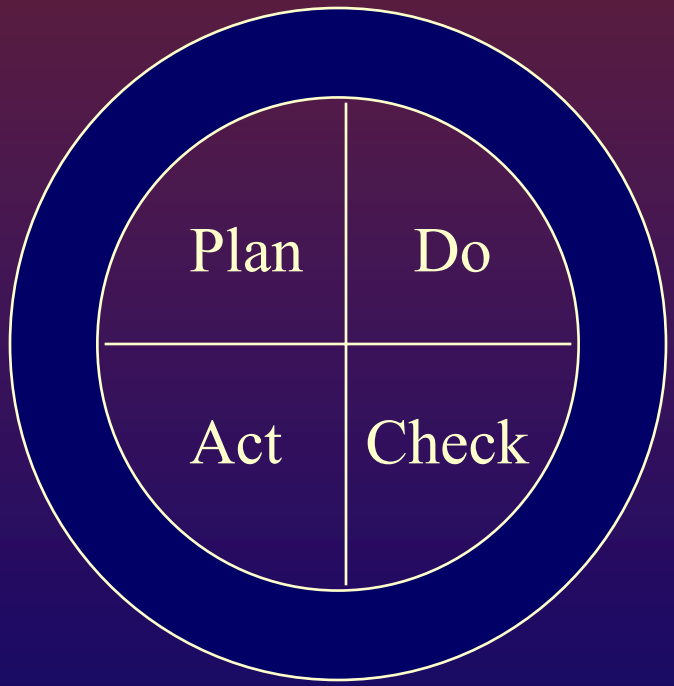


ISO & IEC Comparison

IEC Model



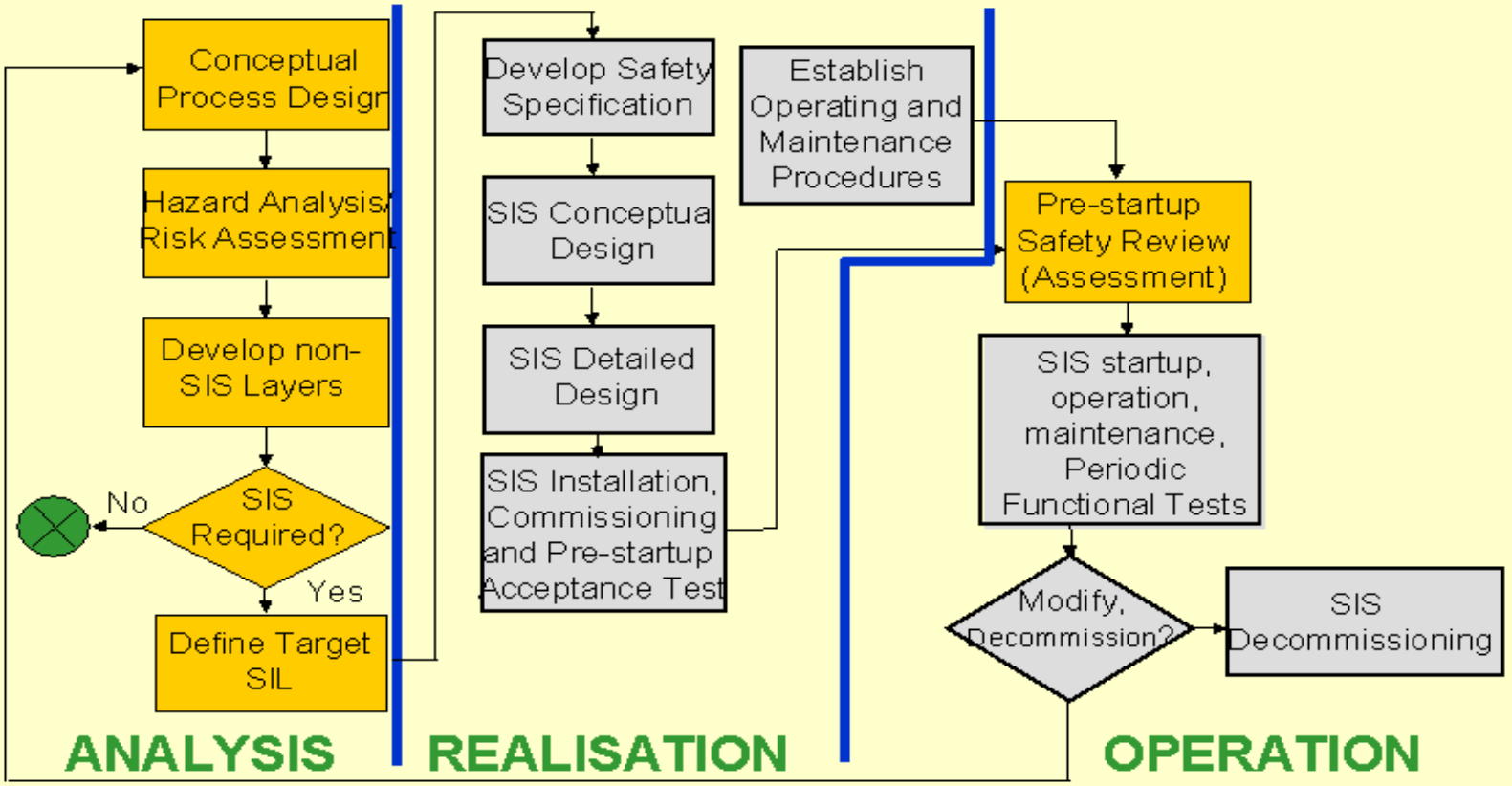
ISO Model



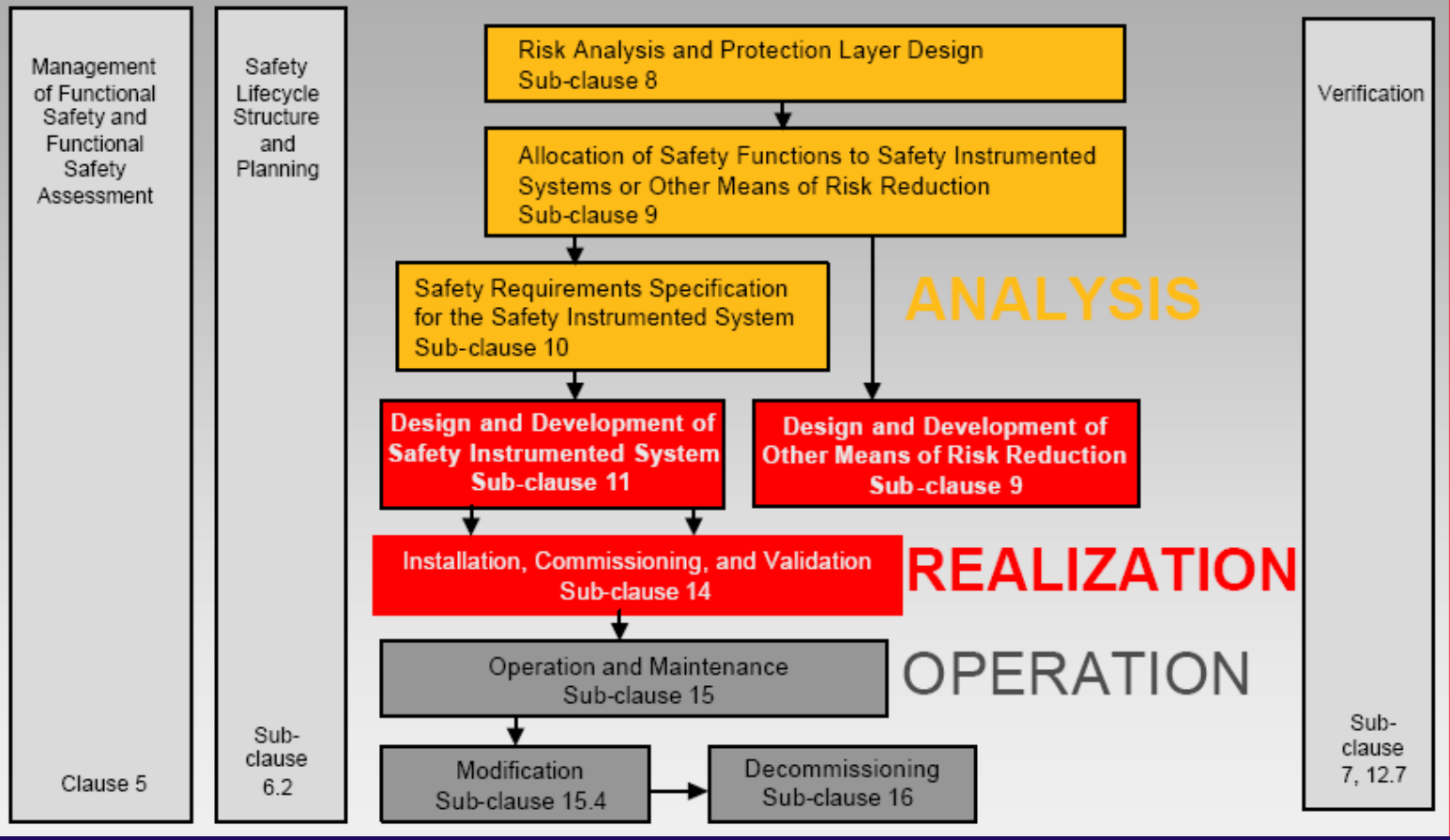
Safety Lifecycle Model

- Divided into three phases
  - Analysis Phase - the problem is identified and assessed
  - Realization Phase – the problem is solved and verified
  - Operational Phase – the solution is put into use

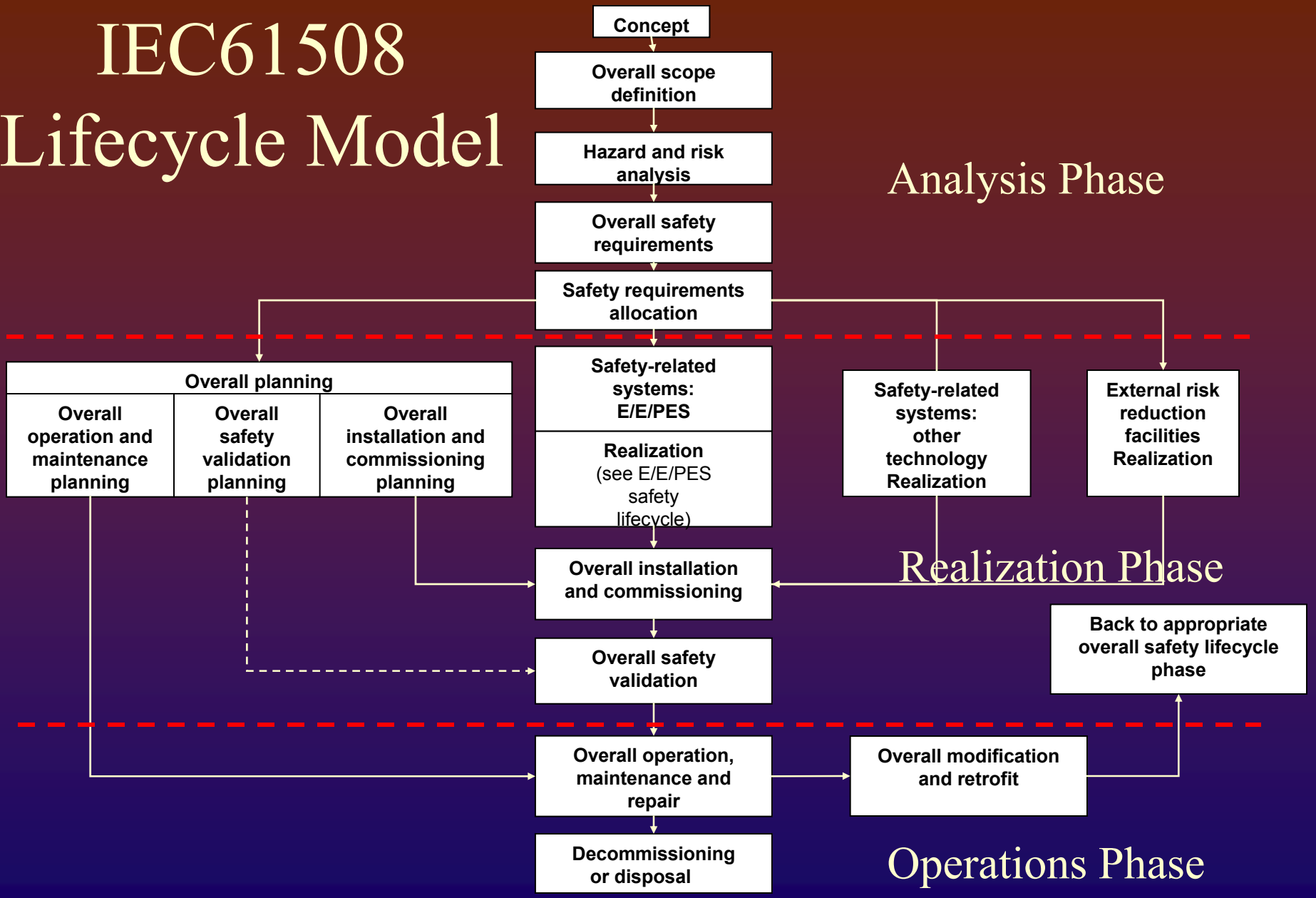
ISA 84.01 Safety Lifecycle



IEC 61511 Safety Life Cycle



IEC61508 Lifecycle Model



Analysis Phase

- Concept
  - Develop an understanding of the equipment under control & its environment (physical & legal)
  - Determine likely hazard sources
  - Collect info on determined hazards (toxicity, explosion)
  - Hazard interaction with other equipment
- Scope Definition
  - Determine process/system boundaries
  - Determine the scope of hazards

Analysis Phase

- Scope Definition
  - Determine the physical equipment to be included in hazard/risk analysis
  - Determine the subsystems associated w/ the hazards
  - Determine what external events will be included
  - Determine types of accident-initiating events

Analysis Phase (continued)

- Hazard & Risk Analysis
  - Develop hazards list & events
    - Includes fault conditions & misuse
    - Abnormal & infrequent operation modes
  - Determine event sequences
  - Determine the likelihood & consequences for each event
  - Evaluate the risk

Analysis Phase (continued)

- Overall Safety Requirements
  - Specify necessary safety functions
    - Functions will not be defined in technology-specific terms
  - Determine necessary risk reduction
    - Qualitative or quantitative
  - Determine safety integrity requirement for each safety function
    - This is an interim stage toward determining SILs

Analysis Phase (continued)

- Safety Requirements Allocation
  - Specify safety-related systems to be used
    - External risk reduction facilities
    - E/E/PE safety-related systems
    - Other technology safety-related systems
  - Allocate safety integrity level to each E/E/PE safety-related system
    - Done after taking into account risk reductions from external risk facilities and other technology safety-related systems
  - Ends with a Safety Requirements Specification document

Realization Phase

- Technology & Architecture selections
- Determine test philosophy
- Perform reliability and safety evaluation to determine if you met your target SIL requirement
- Develop SIS conceptual design
- Prepare detailed design document (wiring diagrams; installation plans, etc.)
- Install system, commission, & perform acceptance testing

Operations Phase

- Design Validation
  - ✓ Does the system solve the problems identified during the hazard analysis?
  - ✓ Have all necessary design steps been carried out successfully?
  - ✓ Has the design met the target SIL for each safety instrumented function?
  - ✓ Have the maintenance procedures been created and verified?
  - ✓ Is there a management of change procedure in place?
  - ✓ Are operators and maintenance personnel qualified and trained?

Operations Phase

- Yes? - May proceed with operations
- Lifecycle continues with evaluations of system modifications and decommissioning activities
- Validation reviews the safety lifecycle activities and ensures that all steps were carried and documentation is in place

Summary

- The safety lifecycle was created to
  - help safety instrumented system designers build safer systems
  - help create more cost effective systems
- Various lifecycle models exist but contain similar steps
- Documentation at every step is key to managing your system effectively